

1 BRIAN J. STRETCH (CABN 163973)
2 United States Attorney

3 BARBARA VALLIERE (CABN 147374)
4 Chief, Criminal Division

5 WILLIAM FRENTZEN (LABN 24421)
6 Assistant United States Attorney

7 450 Golden Gate Avenue, Box 36055
8 San Francisco, California 94102-3495
Telephone: (415) 436-6959
Fax: (415) 436-7234
William.Frentzen@usdoj.gov

9 Attorneys for United States of America

10 UNITED STATES DISTRICT COURT

11 FOR THE NORTHERN DISTRICT OF CALIFORNIA

12 SAN FRANCISCO DIVISION

13 UNITED STATES OF AMERICA,

) No. CR 16-00227 RS

14 Plaintiff,

) AFFIDAVIT OF AUSA WILLIAM

15 v.

) FRENTZEN IN SUPPORT OF REQUEST FOR

16 BTC-E, and

) EXTRADITION OF ALEXANDER VINNIK

17 ALEXANDER VINNIK,

18 Defendants.

)

)

)

)

)

22 I, William Frentzen, being duly sworn, depose and state:

23 1. I am a citizen of the United States of America, and a resident of the state of California.

24 2. I graduated from Tulane University School of Law, New Orleans, Louisiana, in 1996.

25 From 1996 to 2006, I served as a federal prosecutor in different offices and jurisdictions, including
26 Washington, D.C. From 2006 to the present, I have been employed by the United States Department of
27 Justice as an Assistant United States Attorney for the Northern District of California. In that capacity, I
28 am responsible for preparing and prosecuting criminal cases against persons charged with criminal

FILED

AUG 09 2017

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SEALED BY ORDER
OF COURT

1 violations of the laws of the United States. During my practice as an Assistant United States Attorney,
2 I have become knowledgeable about the criminal laws and procedures of the United States.

3. I am currently assigned as the Senior Trial Counsel for the United States Attorney's
4 Office. Through this case and prior cases, I am particularly knowledgeable in the area of the law
5 relating to violations of the money laundering laws involving digital currency such as Bitcoin, including
6 the crimes involved in this case.

7. In the course of my duties, I have become familiar with the charges and evidence in the
8 case of *United States v. BTC-e and Alexander Vinnik*. This prosecution arose from an investigation by
9 Internal Revenue Service Criminal Investigations ("IRS-CID"), United States Department of Homeland
10 Security, Homeland Security Investigations ("HSI"), the Federal Bureau of Investigation ("FBI"),
11 United States Secret Service ("USSS"), and the Federal Deposit Insurance Corporation Office of
12 Inspector General ("FDIC OIG") into (1) the unregistered operation of BTC-e as a money transmitting
13 business; (2) the knowing laundering of money by BTC-e; and (3) the money laundering of proceeds by
14 Vinnik from a computer intrusion, or "hack" of Mt. Gox, a well-known and now failed digital currency
15 exchange.

PROCEDURAL HISTORY OF THE CASE

5. On May 31, 2016, a federal Grand Jury returned an Indictment under seal in San
Francisco in the Northern District of California in Criminal Case 16-227 RS (indicating that the case is
before the Honorable Richard Seeborg, United States District Judge for the Northern District of
California) charging BTC-e, Alexander Vinnik ("VINNIK"), and three other individuals with operating
an unlicensed money transmitting business and conspiracy to launder money.

6. On January 17, 2017, a federal Grand Jury returned a Superseding Indictment under seal
in San Francisco in the Northern District of California in Criminal Case No. 16-227 RS. On January
17, 2017, the Honorable Sallie Kim, United States Magistrate Judge, signed a warrant for VINNIK's
arrest based upon the Superseding Indictment. This warrant is attached hereto as Exhibit A. The
Superseding Indictment replaces the previous indictment in this case. That indictment charges BTC-e
and VINNIK with operating an unlicensed money transmitting business and conspiracy to launder
money as well as charging VINNIK with multiple counts of money laundering the proceeds from an

1 intrusion (hack) of a digital currency exchange called Mt. Gox. A copy of the Superseding Indictment
2 is attached hereto as Exhibit B. VINNIK has never appeared in the Northern District of California to
3 answer the charges in this case.

4 THE CHARGING PROCESS

5 7. Under United States law, the filing of an indictment may take place after it is returned by
6 a grand jury. Institutionally, a grand jury, though an arm of the court, is an independent body
7 composed of private citizens not fewer than 16 and not more than 23 people whom the United
8 States District Court selects at random from the residents of the judicial district in which the court
9 resides. The purpose of the grand jury is to review the evidence of crimes presented to it by United
10 States law enforcement authorities. After independently reviewing this evidence, each member of the
11 grand jury must determine whether there is enough credible evidence to believe that a crime has been
12 committed and that a particular person committed that crime. If at least 12 jurors determine that it is
13 more likely than not that a particular person committed the crime, the grand jury may return an
14 indictment. An indictment is a formal written accusation that charges the particular person, now a
15 defendant, with a crime, identifies the specific laws that the defendant is accused of violating, and
16 specifies the date and place where the charged crime occurred. The indictment by the grand jury is
17 filed with the United States District Court. After an indictment has been returned, the same grand jury
18 or a different grand jury can return additional, superseding indictments in the same proceeding charging
19 the same or additional crimes.

20 8. In addition to imprisonment and a criminal fine, United States law provides for the
21 seizure and forfeiture of property of the defendant that constitutes the proceeds of fraud schemes. A
22 criminal forfeiture may be alleged in an indictment, along with substantive crimes, only if the grand
23 jury finds enough credible evidence to believe that the property is forfeitable. Under United States law,
24 asset forfeiture is not a substantive offense or an element of the crime, but is a required part of
25 sentencing that the court must impose upon conviction for certain criminal offenses. A criminal
26 forfeiture allegation in the indictment simply provides the defendant with notice that the United States
27 will seek to forfeit certain property, or a money judgment and substitute assets, if the defendant is
28 convicted of the particular offense.

1 THE CHARGES AND PERTINENT UNITED STATES LAW

2 9. On January 17, 2017, a federal grand jury, sitting in the Northern District of California,
3 approved and filed a Superseding indictment charging BTC-e and VINNIK with the following criminal
4 offenses:

5 a. Count One: Illegally operating an unlicensed money transmitting business, in violation of
6 Title 18, United States Code, Section 1960. By operating a money transmitting business that
7 handled money from the United States and did not register with the Financial Crimes
8 Enforcement Network (“FinCEN”), BTC-e and VINNIK avoided controls that they would have
9 to implement to prevent the laundering of illegal proceeds through the digital currency exchange
10 BTC-e. An “unlicensed money transmitting business” means a money transmitting business
11 affecting interstate or foreign commerce that either (1) operated without appropriate license
12 registration under section 5330 of title 31, United States Code, and regulations under that statute
13 (including the requirement to implement proper anti-money laundering and know your customer
14 processes), or (2) that involved transmission of funds know to have been derived from a
15 criminal offense and intended to be used to promote and support unlawful activity. VINNIK is
16 also charged in Count One with committing this offense as a principle and as an aider and
17 abettor under Title 18 United States Code, Section 2. The aiding and abetting statute (Title 18,
18 United States Code, Section 2) states that whoever commands, procures, assists in, or causes the
19 commission of a crime shall be held accountable and punished in the same manner as the
20 principal, or the person who actually carried out the task. This means that VINNIK’s guilt also
21 may be proved even if he did not personally perform every act involved in the commission of
22 the crime charged. The law recognizes that, ordinarily, anything a person can do for himself
23 may also be accomplished through the direction of another person as an agent, or by acting
24 together with, or under the direction of, another person or persons in a joint effort. So, if the
25 acts or conduct of an agent, employee, or other associate of the defendant were willfully
26 directed or authorized by the defendant, or if the defendant aided and abetted another person by
27 willfully joining together with that person in the commission of a crime, then the law holds the
28 defendant responsible for the conduct of that other person just as though the defendant had

1 engaged in such conduct himself. The maximum penalty for a violation of the offense charged
2 in Count One is 5 years of imprisonment; a fine of \$250,000; 3 years of supervised release; and
3 a mandatory \$100 special assessment.

4 b. Count Two: Conspiracy to commit money laundering in violation of Title 18, United States
5 Code, Section 1956(h). By operating BTC-e without any safeguards for money launderers,
6 VINKI and his fellow managers and conspirators knew and agreed that they were creating a
7 platform for money laundering throughout the world, including in the United States. Under
8 United States law, a conspiracy is an agreement to commit one or more criminal offenses. The
9 agreement on which the conspiracy is based need not be expressed in writing or in words, but
10 may simply be a tacit understanding by two or more persons to do something illegal. A person
11 may become a member of a conspiracy without full knowledge of all the details of the unlawful
12 scheme or the identities or specific roles of all the other members of the conspiracy. Ultimately,
13 a person is guilty of conspiracy if (1) that person entered into an agreement to violate the law
14 with at least one other person; (2) that person was aware of the purpose of the agreement and
15 deliberately and voluntarily joined in the agreement; and (3) during the existence of the
16 agreement one of the members of the agreement performed an act to advance the purpose of the
17 agreement. Once part of a conspiracy, a conspirator can be held criminally responsible for all
18 reasonably foreseeable actions taken by other conspirators in furtherance of the criminal
19 partnership. The crime of conspiracy is an independent offense, separate and distinct from the
20 commission of any specific substantive crime. The maximum penalty for a violation of the
21 offense charged in Count Two is 20 years of imprisonment; a fine of \$500,000; 3 years of
22 supervised release; and a mandatory \$100 special assessment.

23 c. Counts Three through Nineteen: Money laundering, in violation of Title 18, United States
24 Code, Sections 1956(a)(1)(A)(i) and (a)(1)(B)(i) and 2. VINKI used a digital currency
25 exchange called Tradehill to launder digital currency stolen through illegal computer access by
26 fraud and conducted financial transactions in order to disguise and conceal the ownership and
27 source of the proceeds. Specifically, the essential elements for this money laundering offense is
28 as follows: (1) that VINKI conducted a financial transaction involving property that

1 represented the proceeds of an illegal computer intrusion; (2) VINNIK knew that the property
2 represented the proceeds of illegal activity; and (3) the defendant acted with the intent to
3 promote the carrying on of illegal computer intrusion, or VINNIK acted with the knowledge that
4 the transaction was designed in whole or in part to conceal or disguise the nature, location,
5 source, ownership, or control of the proceeds of an illegal computer intrusion or that VINNIK
6 aided and abetted that crime. The crime of illegal computer intrusion consists of the following
7 elements: (1) a person knowingly accessed without authorization a computer used in or affecting
8 interstate or foreign commerce; (2) the person did so with the intent to defraud; (3) by accessing
9 the computer without authorization, the person furthered the intended fraud; and (4) the
10 defendant by accessing the computer without authorization obtained anything of value. The
11 maximum penalty for each violation of the offense charged in Counts Three through Nineteen is
12 20 years of imprisonment; a fine of \$500,000; 3 years of supervised release; and a mandatory
13 \$100 special assessment.

14 d. Counts Twenty and Twenty-One: Money laundering, in violation of Title 18, United States
15 Code, Sections 1957 and 2. VINNIK used a digital currency exchange called Tradehill to
16 launder digital currency stolen through illegal computer access by fraud and conducted
17 monetary transactions in excess of \$10,000 with the proceeds. Specifically, the essential
18 elements of this money laundering offense is as follows: (1) VINNIK knowingly engaged in a
19 monetary transaction; (2) VINNIK knew the transaction involved criminally derived property;
20 (3) the property had a value greater than \$10,000; and (4) the property was, in fact, derived from
21 illegal computer intrusion or that VINNIK aided and abetted that crime. The maximum penalty
22 for each violation of the offense charged in Counts Twenty and Twenty-One is 10 years of
23 imprisonment; a fine of \$500,000; 3 years of supervised release; and a mandatory \$100 special
24 assessment.

25 10. The United States requests the extradition of VINNIK for all of these offenses. Each
26 count charges a separate offense. Each offense is punishable under a statute that (1) was the duly
27 enacted law of the United States at the time the offense was committed, (2) was the duly enacted law of
28 the United States at the time the indictment was filed, and (3) is currently in effect. Each offense is a

1 felony offense punishable under United States law by one year or more of imprisonment. I have
2 attached copies of the pertinent sections of these statutes and the applicable penalty provisions to this
3 affidavit as Exhibit C.

4 11. I have also included, as part of Exhibit C, the true and accurate text of 18 U.S.C. § 3282,
5 which is the statute of limitations for the crimes charged in the indictment. The statute of limitations
6 requires that a defendant be formally charged within five years of the date on which the offense or
7 offenses were committed. Once an indictment has been filed in a federal district court, as with the
8 charges against VINNIK, the statute of limitations is tolled and no longer runs. The reason for this is to
9 prevent a criminal from escaping justice simply by fleeing the country and remaining a fugitive for a
10 long period of time.

11 12. I have reviewed the applicable statute of limitations. Because the applicable statute of
12 limitations is five years and the indictment, which charges criminal violations beginning on January 23,
13 2012, and continuing through the date of the indictment, January 17, 2017, was filed in January 2017,
14 VINNIK was formally charged within the prescribed five-year time period. The prosecution of the
15 charges in this case, therefore, is not barred by the statute of limitations.

16 13. VINNIK has not been prosecuted or convicted for any of the offenses for which
17 extradition is sought, nor has he been ordered to serve any sentence for any of the offenses that form the
18 basis of this request.

SUMMARY OF THE FACTS

14. BTC e began functioning in 2011 as a digital currency exchanger. It functions in the
United States and around the world through the domain btc-e.com. BTC-e serves all functions of a
digital currency exchange, including transmitting money in the form of many varieties of digital
currency (Bitcoin, Ethereum, Dogecoin, Litecoin, etc.). BTC-e allows customers to convert digital
currency to fiat currency (U.S. dollars, euros, rubles, etc.) and the reverse. BTC-e has never been
registered with FinCEN. BTC-e has never had any effective methods to determine the true identities of
its customers. BTC-e has never reported suspicious activity taking place on its site. As a result, BTC-e
knowingly established methods of serving as a money transmitting business attractive to criminal
proceeds. In 2013, another exchange, Liberty Reserve, was known for facilitating criminal digital

1 currency transactions. As a result of United States law enforcement actions, Liberty Reserve was
2 charged with crimes, taken offline, and responsible individuals were arrested and prosecuted.
3 Immediately following the collapse of Liberty Reserve, BTC-e saw a large influx of additional
4 customers and use. Effectively, the criminal element that had used Liberty Reserve moved to use BTC-
5 e, often with the same online name and/or email identifiers. BTC-e established itself as the "go to"
6 exchange for criminal proceeds and profited greatly from that business.

7 15. Evidence connects VINNIK as an owner and manager of BTC-e. Although VINNIK has
8 attempted to establish nominees and aliases to try to shield himself from responsibility for BTC-e and
9 its activities, he is clearly the operator of BTC-e. Primarily, VINNIK has been tied to BTC-e through
10 his control of various online accounts and email addresses that continuously resurface as controlling
11 accounts for the operation of BTC-e. The links between VINNIK, BTC-e, and the proceeds from BTC-
12 e are discussed in detail in the Affidavit of Special Agent Michael Delaney from Homeland Security
13 Investigations, with which I am familiar and which I incorporate into this Affidavit.

14 16. Finally, tracing of bitcoin coming from the hack of Mt. Gox links VINNIK to the
15 laundering of the proceeds from that hack through both BTC-e and through Tradehill, a now defunct
16 digital currency exchange that was based in San Francisco, California, within the Northern District of
17 California.

18 17. Attached as Exhibit D is the affidavit of HSI Special Agent Michael Delaney which
19 further details the evidence against VINNIK.

20 IDENTIFICATION

21 18. VINNIK was born in Russia on REDACTED . He is described as a white male,
22 medium height and weight. Attached to the affidavit of HSI Special Agent Michael Delaney as Exhibit
23 1 are photographs of VINNIK's current and previous passport photographs, both of which were
24 obtained from VINNIK's personal email account, wmewme@gmail.com, and Hyatt Hotels
25 Corporations.

26 //

27 //

28 //

CONCLUSION

19. I have thoroughly reviewed the affidavit of Special Agent Delaney and the evidence in this case and attest that this evidence indicates that he is guilty of the offenses charged in the Indictment.

20. If Greek authorities or a Greek court believe that additional information is needed in support of this extradition request after the submission of this request, the United States (through the Department of Justice, Office of International Affairs) hereby requests, pursuant to the 1931 U.S.-Greece Extradition Treaty and the 2006 U.S.-Greece Extradition Protocol, that it be given notice of any perceived deficiencies immediately, and that the United States be given an opportunity to supplement its request for extradition within a reasonable time period.

Executed this 9th day of August, 2017, at San Francisco, California, United States of America.

WILLIAM FRENTZEN
Assistant United States Attorney

Signed and sworn to before me this 9th day of August, 2017, at San Francisco, California.

HONORABLE RICHARD SEEBORG
UNITED STATES DISTRICT JUDGE

1. LIST OF EXHIBITS

Exhibit A: A certified copy of the arrest warrant.

Exhibit B: A certified copy of the indictment.

Exhibit C: Excerpts of the following statutes:

Title 18, United States Code, Section 1960;

Title 18, United States Code, Section 1961;

Title 18, United States Code, Section 1956;

Title 18, United States Code, Section 1957;

Title 18, United States Code, Section 2;

Title 18, United States Code, Section 982;

Title 18, United States Code, Section 981;

Title 21, United States Code, Section 853;

Fed. R. Crim. P. 32.2(a);

Title 18, United States Code, Section 3282;

Title 31, United States Code, Section 5330; and

FinCEN Guidance - FIN-2013-G001.

Exhibit D: Affidavit of HSI Special Agent Michael Delaney.

{

(

A

EXHIBIT A

Arrest Warrant

SEALED BY ORDER
OF COURT

AO 442 (Rev. 01/09) Arrest Warrant

RECEIVED
UNITED STATES MARSHAL

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT
OF CALIFORNIA
Northern District of California

United States of America

v.

HTC-F.A.K/A CANTON BUSINESS CORPORATION and ALEXANDER VINNIK
Defendants

Case No. CR 16-00227 SI

ARREST WARRANT

To: Any authorized law enforcement officer

I hereby certify that the annexed
instrument is a true and correct copy
of the original on file in my office
ATTEST:SUSAN Y SOONG
Clerk, U.S District Court
Northern District of CaliforniaBy Susan Y Soong
Deputy Clerk
Date 8/8/17

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) ALEXANDER VINNIK

who is accused of an offense or violation based on the following document filed with the court:

- Indictment Superseding Indictment Information Superseding Information Complaint
 Probation Violation Petition Supervised Release Violation Petition Violation Notice Order of the Court

This offense is briefly described as follows:

- 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;
 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;
 18 U.S.C. § 1956(a)(1) - Money Laundering;
 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and
 18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

Date: 01/17/2017Sallie Klm
Issuing officer's signatureCity and state: San Francisco, California

United States Magistrate Judge Sallie Klm

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____

Date: _____

Sallie Klm
Arresting officer's signature

Printed name and title

{

(

B

C

E

1 EXHIBIT B
2
3
4
5
6
7
8
9
10
11
12 **Superseding Indictment**
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

UNITED STATES OF AMERICA,

SEALED V.
BY COURT ORDER

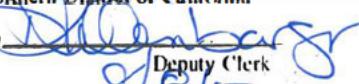
CR16-0227-SI

BTC-E, A/K/A CANTON BUSINESS CORPORATION
and ALEXANDER VINNIK,

I hereby certify that the annexed
instrument is a true and correct copy
of the original on file in my office.

ATTEST:

SUSAN Y. SOONG
Clerk, U.S. District Court
Northern District of California

By 
Deputy Clerk
Date 8/6/17

DEFENDANT(S).

SUPERSEDING INDICTMENT

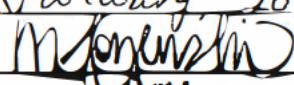
18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;
18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;
18 U.S.C. § 1956(a)(1) - Money Laundering;
18 U.S.C. § 1957 - Unlawful Monetary Transactions; and
18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

A true bill.


Foreman

Filed in open court this 17th day of

January, 2017


SALLIE KIM
United States Magistrate Judge

Clerk

NO BAIL WARRANT
for Alexander Vinnik

NO PROCESS for BTC-E

Bail, \$ _____



AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURTBY: COMPLAINT INFORMATION INDICTMENT SUPERSEDING**OFFENSE CHARGED**

18 U.S.C. § 1960 Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. §§ 982(a)(1) Criminal Forfeiture

- Petty
 Minor
 Misdemeanor
 Felony

PENALTY: Please see attachment.

SEALED BY COURT ORDER**PROCEEDING**

Name of Complainant Agency, or Person (& Title, if any)

Internal Revenue Service

person is awaiting trial in another Federal or State Court, give name of court

this person/proceeding is transferred from another district per (circle one) FRCrP 20, 21, or 40. Show District

this is a reprocution of charges previously dismissed
 which were dismissed on motion of:

U.S. ATTORNEY DEFENSE

this prosecution relates to a pending case involving this same defendant

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

SHOW DOCKET NO.
{

MAGISTRATE CASE NO.
{

Name and Office of Person Furnishing Information on this form BRIAN J. STRETCH

U.S. Attorney Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned)

WILLIAM FRENTZEN

PROCESS:

SUMMONS NO PROCESS* WARRANT

Bail Amount: _____

If Summons, complete following:

Arraignment Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: _____ Before Judge: _____

Comments:

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

BTC-E, A/K/A CANTON BUSINESS CORPORATION

DISTRICT COURT NUMBER

CR 16 00227 SI

JAN 17 2017
CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SUSAN Y. SOONG

DEFENDANT

IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

- 1) If not detained give date any prior summons was served on above charges

- 2) Is a Fugitive

- 3) Is on Bail or Release from (show District)

IS IN CUSTODY

- 4) On this charge

- 5) On another conviction

} Federal State

- 6) Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer Yes } If "Yes"
 been filed? No } give date
 filed _____

DATE OF ARREST Month/Day/Year

Or... If Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

This report amends AO 257 previously submitted

ATTACHMENT TO PENALTY SHEET

BTC-E, A/K/A CANTON BUSINESS CORPORATION

COUNT ONE: (18 U.S.C. §1960 Operation of an Unlicensed Money Service Business)

5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) Criminal Forfeiture)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: COMPLAINT INFORMATION INDICTMENT
 SUPERSEDING

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. §§ 982(a)(1) Criminal Forfeiture

PENALTY: Please see attachment.

- Petty
- Minor
- Misdemeanor
- Felony

**SEALED
BY COURT ORDER**

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Internal Revenue Service

person is awaiting trial in another Federal or State Court,
give name of court

this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a reprocution of charges previously dismissed which were dismissed on motion of:

U.S. ATTORNEY DEFENSE

this prosecution relates to a pending case involving this same defendant

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person
Furnishing Information on this form BRIAN J. STRETCH

U.S. Attorney Other U.S. Agency

Name of Assistant U.S.
Attorney (if assigned)

WILLIAM FRENTZEN

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

SUMMONS NO PROCESS* WARRANT

If Summons, complete following:

Arraignment

Bail Amount:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET

ALEXANDER VINNIK

COUNT ONE: (18 U.S.C. §1960 – Operation of an Unlicensed Money Service Business)

5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) Criminal Forfeiture)

1 BRIAN J. STRETCH (CABN 163973)
2 United States Attorney
3
4
5

FILED
JUL 11 2017 P 4:38
CLERK, U.S. DISTRICT COURT
NO. 3:16-cr-00227

6 **SEALED**
7 **BY COURT ORDER**

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA, } UNDER SEAL
12 Plaintiff, } CASE NO. CR 16-00227 SI
13 v. } VIOLATIONS: 18 U.S.C. § 1960 Operation of an
14 BTC-E, A/K/A CANTON BUSINESS } Unlicensed Money Service Business; 18 U.S.C.
15 CORPORATION, } § 1956(h) – Conspiracy to Commit Money
16 and } Laundering; 18 U.S.C. § 1956(a)(1) Money
17 ALEXANDER VINNIK } Laundering; 18 U.S.C. § 1957 Unlawful Monetary
18 Defendants. } Transactions; 18 U.S.C. § 982(a)(1) Criminal
 } Forfeiture
 } SAN FRANCISCO VENUE

19 SUPERSEDING INDICTMENT

20 The Grand Jury charges:

21 INTRODUCTORY ALLEGATIONS

22 At all times relevant to this Indictment:

23 1. Since at least approximately 2011 through and including the present, both dates being
24 approximate and inclusive, the defendant BTC-e operated as one of the world's largest and most widely
25 used digital currency exchanges. Since its inception, BTC-e processed several billion dollars worth of
26 monetary exchanges. BTC-e was an exchange for cybercriminals worldwide, and one of the principal
27 entities used to launder and liquidate criminal proceeds from digital currencies, including Bitcoin, to fiat
28

1 currencies,¹ including U.S. dollars, Euros, and Rubles. At all relevant times, the defendant
 2 ALEXANDER VINNIK, together with individuals known and unknown, directed and supervised BTC-
 3 e's operations and finances.

4 2. BTC-e was an international money-laundering scheme that, by virtue of its business
 5 model, catered to criminals – and to cybercriminals in particular. Through VINNIK's efforts, BTC-e
 6 emerged as one of the principal means by which cyber criminals around the world laundered the
 7 proceeds of their illicit activity. BTC-e facilitated crimes, including computer hacking and ransomware,
 8 fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.

9
 10 3. BTC-e lacked basic anti-money laundering controls and policies and, as such, was
 11 attractive to those who desired to conceal criminal proceeds as it made it more difficult for law
 12 enforcement to trace and attribute funds.

13
 14 4. Since its founding, BTC-e received criminal proceeds of numerous computer intrusions
 15 and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics
 16 distribution rings. Among other things, BTC-e accounts received substantial proceeds from the hack of
 17 the now-defunct Mt. Gox digital currency exchange and also received a substantial portion of the
 18 criminal proceeds from one of the largest ransomware schemes, CryptoWall.

19
 20 5. As described further below, the defendants and their co-conspirators, including those
 21 known and unknown to the Grand Jury, intentionally created, structured, and operated BTC-e as a
 22 criminal business venture, one designed to help criminals launder their proceeds and one they
 23 themselves used to launder criminal proceeds. The defendants thus attracted and maintained a customer
 24 base that was heavily reliant on criminals.

25 6. Despite doing substantial business in the United States, BTC-e was not registered as a

26
 27 ¹ Fiat currency is simply a currency established by government regulation or law, e.g. U.S.
 28 Dollars, Euros, Japanese Yen, British Pounds, Russian Rubles, Chinese RMB, etc.

1 money services business with the United States Department of the Treasury's Financial Crimes
2 Enforcement Network ("FinCEN"), as federal law requires. As described further below, BTC-e had no
3 meaningful anti-money laundering processes in place and lacked an effective anti-money laundering
4 program, as federal law also requires.

7. This was in contrast to other registered digital currency exchanges that, through their anti-money laundering programs, strove to avoid having their platforms used for criminal activity. Most of those exchanges described their operations down to listing the names, photos, and backgrounds of their management, the location of their businesses, and their regulatory compliance policies.

8. BTC-e relied on the use of shell companies and affiliate entities that were similarly unregistered with FinCEN and lacked basic anti-money laundering and “Know Your Customer” policies. These entities catered to an online and worldwide customer base, and electronically “muled” fiat currency in and out of BTC-e. BTC-e’s own website stated it was located in Bulgaria, yet simultaneously stated it was subject to the laws of Cyprus. Meanwhile, BTC-e’s managing shell company, CANTON BUSINESS CORPORATION, was based in the Seychelles but affiliated with a Russian phone number, and its web domains were registered to shell companies in countries including Singapore, the British Virgin Islands, France, and New Zealand.

BACKGROUND

9. Bitcoin is a form of decentralized, convertible digital currency that existed through the use of an online, decentralized ledger system.² Bitcoin is just one of many forms of digital currency. There are many others, including litecoin, ethers, worldcoin, and dogecoin. However, bitcoin has the largest market capitalization of any present form of decentralized digital currency.

10. While bitcoin mainly exists as an Internet-based form of currency, it is possible to “print out” the necessary information and exchange bitcoin via physical medium. The currency is not issued

² Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

1 by any government, bank, or company, but rather is generated and controlled through computer software
 2 operating via a decentralized network. To acquire bitcoin, a typical user will purchase them from a
 3 Bitcoin seller or “exchanger.” It is also possible to “mine” bitcoin by verifying other users’ transactions.
 4 Bitcoin is just one form of digital currency, and there are a significant number of other varieties of
 5 digital currency.

6 11. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its
 7 value from government regulation or law), or other convertible digital currencies. When a user wishes
 8 to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency,
 9 often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding
 10 quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will
 11 then typically attempt to broker the purchase with another user of the exchange that is trying to sell
 12 bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a
 13 seller, then the transaction can be completed.

14 12. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user’s bitcoin
 15 address. The bitcoin address is somewhat analogous to a bank account number, and is comprised of a
 16 case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can
 17 then conduct transactions with other Bitcoin users, by transferring bitcoin to their bitcoin addresses, via
 18 the Internet.

19 13. Little to no personally identifiable information about the payer or payee is transmitted in
 20 a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public
 21 key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address.
 22 Only the bitcoin address of the receiving party and the sender’s private key are needed to complete the
 23 transaction. These two keys by themselves rarely reflect any identifying information.

24 14. All bitcoin transactions are recorded on what is known as the blockchain. This is
 25 essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing,
 26 and updates approximately six times per hour. The blockchain records every bitcoin address that has
 27 ever received a bitcoin and maintains records of every transaction for each bitcoin address.

28 15. Digital currencies, including bitcoin, have many known legitimate uses. However, much

1 like cash, bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the
 2 ease with which bitcoin can be used to move funds with high levels of anonymity. As is demonstrated
 3 herein, however, in some circumstances bitcoin payments may be effectively traced by analyzing the
 4 blockchain.

5 BTC-E OVERVIEW

6 16. BTC-e was founded in or about 2011. In the years it operated, BTC-e has served
 7 approximately 700,000 users worldwide, including numerous customers in the United States and
 8 customers in the Northern District of California. BTC-e touts itself as “a platform for individuals
 9 interested in buying and selling bitcoin using an assortment of world currencies;” in other words, a
 10 digital currency exchange.

11 17. Through the work of VINNIK and others known and unknown to the Grand Jury, BTC-e
 12 became one of the primary ways by which cybercriminals around the world transferred, laundered, and
 13 stored the criminal proceeds of their illegal activities. U.S. dollars and Russian rubles were the most
 14 frequently exchanged fiat currencies on the platform, while Bitcoin and litecoin were the most widely
 15 exchanged digital currencies.

16 18. Because such a significant portion of BTC-e’s business was derived from suspected
 17 criminal activity and given its global reach, the scope of the defendants’ unlawful conduct was massive.
 18 During the relevant timeframe from 2011 to December 30, 2016, bitcoin addresses associated with BTC-
 19 e had received over 9.4 million bitcoin. Bitcoin’s rapidly fluctuating exchange rate makes it difficult to
 20 determine the U.S. Dollar value of this quantity of bitcoin over time. However, using today’s bitcoin
 21 exchange rate, the total value of bitcoin received by BTC-e over the course of its operation would be
 22 valued at over \$9 billion. In 2016 alone, BTC-e received over 1.8 million bitcoin, valued at over \$1.7
 23 billion at today’s exchange rate.³

24
 25
 26
 27
 28 ³ This is calculated using the December 30, 2016 bitcoin trading value of approximately \$962 per
 bitcoin. Since August 2011, the Bitcoin market price has fluctuated from a low of roughly \$2 to a high

1 19. Notably, the above figures only include bitcoin exchanged on the BTC-e platform and do
 2 not even include the deposits and withdrawals made in other digital currencies, such as litecoin, nor do
 3 these figures take into account well over a billion dollars' worth of what is known as "BTC-e code."
 4 BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other
 5 BTC-e users.

6 20. BTC-e maintained its servers in the United States. The servers were one of the primary
 7 ways in which BTC-e and the defendants effectuated their operations. BTC-e also used many third-
 8 party companies, including companies within the Northern District of California, to effectuate their
 9 operations and enable them to function.

10 21. At its inception, BTC-e was one of a number of digital currency exchanges. It was
 11 engaged in the same line of business as other online digital currency exchanges in existence at the time,
 12 including Liberty Reserve. Liberty Reserve was a Costa Rica-based centralized digital currency service
 13 that laundered approximately \$6 billion in criminal proceeds. It was shuttered in 2013 when its founder
 14 and six other individuals were charged with conspiracy to commit money laundering and with operating
 15 an unlicensed money transmitting business. Liberty Reserve's website was seized by the U.S.
 16 government.⁴

17 22. There was an overlap between many Liberty Reserve users and BTC-e users. BTC-e
 18 itself was a user of Liberty Reserve.

19 23. Another digital currency exchange in operation between 2011 and 2014 was the MTGOX
 20 Exchange ("Mt. Gox") that was originally founded in San Francisco, but ultimately based in Tokyo,
 21 Japan. In 2014, Mt. Gox collapsed, having been the target of a series of major intrusions that resulted in
 22 thefts totaling several hundred million dollars worth of bitcoin. In 2014, Mt. Gox filed for bankruptcy in
 23

24 of approximately \$1200 per bitcoin and has varied dramatically over time..

25
 26
 27
 28 ⁴ MAYZUS, through its predecessor, UWC FINANCIAL SERVICES, also served as an
 exchanger for Liberty Reserve.

Japan.

24. After the collapse of Liberty Reserve, and with the intrusions and accompanying issues that Mt. Gox experienced, BTC-e rapidly grew. The volume of transactions it performed and its number of users expanded, filling the vacuum left by entities like Liberty Reserve and Mt. Gox.

ENTITIES AND INDIVIDUALS

25. As described further below, BTC-e's money laundering operation was partially enabled and supported by MAYZUS FINANCIAL LTD. a/k/a MAYZUS INVESTMENT COMPANY ("MAYZUS"). MAYZUS enabled a mechanism of moving money internationally centered principally on a core of companies owned by a Russian national. MAYZUS used to be known as UWC FINANCIAL SERVICES ("UWC"), but following the seizure and shuttering of another digital currency exchange, Liberty Reserve, UWC rebranded itself as MAYZUS FINANCIAL LTD.

26. MAYZUS offered a wide range of currency exchange services and provided the ability for fiat currency to be sent – through two online affiliates – to and from BTC-e. BTC-e utilized MAYZUS in lieu of a bank account.

27. MONEY POLO was an online payments system and affiliate of MAYZUS. MONEY POLO was registered in the British Virgin Islands with ties to Cyprus. In order to fund a MONEY POLO account, a user transferred funds to MAYZUS for the benefit of a specific MONEY POLO account number. A MONEY POLO account, in turn, was one of the mechanisms that could be used to fund a BTC-e account.

28. MAYZUS and MONEY POLO enabled BTC-e's operation and its business. Like BTC-e, neither MAYZUS nor MONEY POLO was registered as money service businesses with the United States Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). In or about March 2016, Cyprus's Securities and Exchange Commission fined MAYZUS in connection with legal and regulatory violations stemming from lax anti-money laundering policies.

29. CANTON BUSINESS CORPORATION (“CANTON”) was a shell corporation used as a

front for BTC-e's operations. Like BTC-e, CANTON was not registered with FinCEN. Financial and other records demonstrate that CANTON was synonymous with BTC-e. VINNIK, a Russian national, was a primary beneficial owner of CANTON's financial accounts. Although CANTON's listed business address was in the Seychelles, it operated using a Russian telephone number.

30. Vinnik also operated and controlled multiple BTC-e accounts, including a BTC-e account known as the "WME" account. The "WME" account was tied directly to BTC-e administrator accounts. Numerous withdrawals from BTC-e administrator accounts went directly to bank accounts tied to Vinnik.

31. Another such administrator account associated with Vinnik was the "Vamnedam"⁵ account. The "Vamnedam" account was directly linked to the BTC-e administrative, financial, operational and support accounts, accounts to which only those involved in the operations of the BTC-e enterprise would have had access. Proceeds from well-known hacks and thefts from bitcoin exchanges and users around the world funded the Vamnedam account. Out of the Vamnedam account, large payments were made to accounts associated with Vinnik and others known and unknown to the Grand Jury, including a Russian national hereafter referred to as unindicted CO-CONSPIRATOR X, who is alleged to have access to the Vamnedam account.

BTC-E FUNCTION

32. To use BTC-e, one created an account by accessing the BTC-e website. A user did not need to provide even the most basic identifying information such as name, date of birth, address, or other identifiers. All that BTC-e required was a username, password, and an email address. Unlike legitimate payment processors or digital currency exchangers, BTC-e did not require its users to validate their identity information by providing official identification documents, given that BTC-e did not require an identity at all.

⁵ Vamnedam means "I will not give it to you" in Russian.

1 33. Thus, a user could create a BTC-e account with nothing more than a username and email
2 address, which often bore no relationship to the identity of the actual user. Accounts were therefore
3 easily opened anonymously, including by customers in the United States within the Northern District of
4 California.

5 34. At all times relevant to this Indictment, BTC-e had no anti-money laundering and/or
6 “Know-Your-Customer” (KYC) processes and policies in place. As discussed above, BTC-e collected
7 virtually no customer data at all. Nor did BTC-e or its shell companies ever register with FinCEN or
8 perform these functions on BTC-e’s behalf.

9 35. A user could fund a BTC-e account in numerous different ways. One way involved
10 funding the account with fiat currency that would be converted into digital currency, such as bitcoin.
11 With fiat currency, a user could initiate a wire transfer from a financial institution made directly for the
12 benefit of BTC-e to an account at another financial institution, which was routed to a bank account
13 maintained by one of BTC-e’s shell or affiliated companies. A BTC-e user could also fund an account
14 through the use of a third-party payment system, like MONEY POLO, a third-party entity that
15 maintained a direct relationship with BTC-e. MONEY POLO accounts worked to electronically “mule”
16 fiat currency in and out of BTC-e. Incoming fiat currency was deposited into MAYZUS accounts (using
17 its subsidiary MONEY POLO) to transfer into BTC-e. Outgoing digital currency was exchanged and
18 converted to fiat currency and sent through MONEY POLO accounts benefiting MAYZUS.
19

20 36. Another way involved funding a BTC-e account with a user’s existing digital currency.
21 A user with existing digital currency, such as bitcoin, could fund a BTC-e account directly via bitcoin
22 deposits. BTC-e users could also purchase “BTC-e code” that could be sent and exchanged amongst
23 BTC-e users. BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital
24 currencies to other BTC-e users. This served as another conduit for money laundering as it allowed
25 BTC-e customers to withdraw funds from their BTC-e account and transfer them to other BTC-e users
26
27

1 anonymously.

2 37. BTC-e's business model obscured and anonymized transactions and source of funds. For
 3 example, a BTC-e user could not fund an account by directly transferring money to BTC-e itself, but
 4 rather had to wire funds to one of BTC-e's shells or affiliate entities. Nor could BTC-e users withdraw
 5 funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were
 6 required to make any deposits or withdrawals through the use of third-party "exchangers," thus enabling
 7 BTC-e to avoid collecting any information about its users through banking transactions or other activity
 8 that would leave a centralized financial paper trail.

9 38. Once a user funded an account with BTC-e, the user could then do any number of things:
 10 conduct transactions with other BTC-e users; exchange digital currency into fiat currency; or simply use
 11 BTC-e to store digital currency deposits, much like a bank.

12 39. Like other digital currency exchanges, BTC-e charged transaction fees for their services.
 13 BTC-e charged a percentage fee every time a user transferred funds held in BTC-e to another user
 14 through the BTC-e system. In addition, BTC-e charged a percentage fee every time a user used BTC-e
 15 to exchange digital currency held in a BTC-e account into fiat currency.⁶

16 40. In addition to the fees BTC-e charged, users were charged additional fees by MONEY
 17 POLO and MAYZUS, each taking a percentage of the funds exchanged. These added fees were
 18 associated with getting money in and out of the BTC-e platform through these funding mechanisms,
 19 mechanisms that obfuscated the true sender of the currency.

20 41. Those engaged in criminal activity using BTC-e gravitated to BTC-e because of the site's
 21 lack of anti-money laundering and "Know-Your-Customer" processes in place that could have them
 22 reported to the government. Criminals who used BTC-e to launder funds were also willing to go to the
 23 extra trouble of wiring money offshore to entities that operated through shell companies.

24
 25
 26
 27
 28 ⁶ Likewise, MONEY POLO charged fees in addition to BTC-e's fees when transferring fiat
 currency in and out of BTC-e.

1 42. BTC-e made a series of self-serving public statements, designed at least in part to deflect
2 the attention of law enforcement and regulators. For example, despite advertising on their website that
3 “[w]e require our clients to verify identity by providing [sic] scanned copy of ID and scanned copy of
4 utility bill or a bank statement which should not be older than [sic] 6 month. Copy should be in good
5 resolution and colored,” this process was not in fact followed. As discussed, no customer identification
6 whatsoever was required to set up BTC-e accounts, including BTC-e accounts set up by customers in the
7 Northern District of California.
8

43. Likewise, the BTC-e website advertised that “[w]e don’t accept any more international wire transfers from US Citizens or from US Bank.” This, too, was false. Through its elaborate funding mechanisms, BTC-e did in fact knowingly accept wire transfers from banks in the U.S. and made by U.S. citizens.

BTC-E'S CRIMINAL DESIGN

44. As described above, BTC-e's system was designed so that criminals could accomplish financial transactions with anonymity and thereby avoid apprehension by law enforcement or seizure of funds. BTC-e was in fact thus used extensively for illegal purposes, and, particularly since the collapse of entities like Mt. Gox and Liberty Reserve, it functioned as the exchange of choice to convert digital currency like bitcoin to fiat currency for the criminal world, especially by those who committed their crimes online.

45. The defendants were aware that BTC-e functioned as a money laundering enterprise. Messages on its own forum openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged, and how they used BTC-e to launder funds.

46. BTC-e users established accounts under monikers suggestive of criminality, including monikers such as “ISIS,” “CocaineCowboys,” “blackhathackers,” “dzhacker,” and “hacker4hire.”

47. This is not surprising because criminals used BTC-e to launder criminal proceeds and

1 transfer funds among criminal associates. In particular, it was used by hacking and computer intrusion
2 rings operating around the world to distribute criminal proceeds of their endeavors. It was also used by
3 rings of identity thieves, corrupt public officials, narcotics distribution networks, and other criminals.

4 48. In fact, some of the largest known purveyors of ransomware used BTC-e as a means of
5 storing, distributing, and laundering their criminal proceeds. Ransomware is a criminal scheme in which
6 cybercriminals orchestrate the unwanted malicious download of encryption software on an unsuspecting
7 victim computer. It works as follows: once a victim is infected with the malicious software, often by
8 clicking on a fraudulent email, the ransomware will encrypt multiple file types on victim machines and
9 hold those files for ransom, requiring the victim to pay the administrators of the ransomware scheme in
10 order to have their files decrypted. Victims that pay the ransom are able to decrypt their files by using a
11 stand-alone program provided by the ransomware administrators after the ransom payment has been
12 made. The method of encryption implemented by the ransomware, if properly executed, renders it
13 impossible for victims to decrypt their encrypted files in any other way. The most prevalent payment
14 method accepted by current purveyors of ransomware is bitcoin.
15

16 49. One such ransomware scheme, CryptoWall, was distributed by methods including
17 fraudulent and phishing emails. CryptoWall was one of the most infamous varieties of ransomware and
18 has infected a vast number of computers across the world. During the timeframe relevant to this
19 Indictment, the purveyors of CryptoWall deposited and laundered many hundreds of thousands of
20 dollars' worth of ransom payments into BTC-e.
21

22 50. So, too, did a pair of corrupt U.S. federal agents, Carl Mark Force and Shaun Bridges, use
23 BTC-e to launder their criminal proceeds. Their experience with the criminal underworld taught them
24 that using BTC-e, as opposed to a registered exchange with anti-money laundering policies, would
25 maximize their chances of being able to conceal criminal proceeds. Each therefore sent several hundred
26 thousand dollars in criminal proceeds – derived from crimes ranging from theft of government property
27
28

1 to extortion to the BTC-e platform for laundering.

2 51. BTC-e also served as the receptacle and transmitter of criminal funds from a series of
 3 well-publicized computer intrusions and resulting thefts, including the well-publicized thefts from the
 4 Japan-based Mt. Gox exchange. As discussed below, a sizable portion of the stolen Mt. Gox funds were
 5 deposited into accounts controlled, owned, and operated by BTC-e and by defendant VINNIK and
 6 others known and unknown to the Grand Jury.
 7

8 52. The Mt. Gox exchange was the subject of a series of computer intrusions and resulting
 9 thefts between approximately September 2011 and May 2014, in violation of Title 18, United States
 10 Code, Section 1030(a)(4). Several hundred millions dollars' worth of bitcoin was stolen, including from
 11 numerous customers in the U.S. and within the Northern District of California. After the thefts, some
 12 approximately 530,000 of the bitcoin (worth hundreds of millions of dollars) stolen from Mt. Gox was
 13 deposited into wallets at three different digital currency exchanges: (i) BTC-e; (ii) Trade Hill, another
 14 exchange based in San Francisco; and (iii) back into Mt. Gox into a different Mt. Gox wallet.
 15

16 53. Of this 530,000 bitcoin,⁷ 300,000 of it was sent directly to three separate BTC-e
 17 accounts: "Vamnedam," "Grmbit," and "Petr." These accounts were all linked to each other.

18 54. Meanwhile, blockchain analysis reveals that the stolen Mt. Gox funds that went to Trade
 19 Hill and back into the other Mt. Gox account were controlled by a user who also controlled a BTC-e
 20 account called "WME." At all times relevant to this Indictment, defendant VINNIK exercised control
 21 over the BTC-e "WME" account.
 22

23 55. The "Vamnedain," "Grmbit," "Petr," and "WME" accounts were each directly linked to a
 24 variety of different BTC-e administrative accounts, accounts for which only BTC-e administrators
 25 and/or operators would have had access. The "Vamnedam" account was similarly a
 26
 27

28 7 The amount of bitcoin stolen from Mt. Gox accounted for just under half of the total thefts that
 Mt. Gox suffered.

56. VINNIK, along with others known and unknown, controlled and operated the “Vamnedam” account. Between approximately August 2013 and November 2015, CO-CONSPIRATOR X and identities linked to VINNIK and to BTC-e received direct payments from the “Vamnedam” account to their own personal digital currency accounts at another digital currency exchange, Bitstamp. These bitcoin were then exchanged into fiat currency and sent to bank accounts in Cyprus and Latvia tied to VINNIK and other identities associated with VINNIK and BTC-e.

STATUTORY ALLEGATIONS

COUNT ONE: (18 U.S.C. § 1960 Operation of an Unlicensed Money Transmitting Business)

57. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein as if set forth in full.

58. Title 18, United States Code, Section 1960, makes it a crime to operate an unlicensed
money transmitting business. The term money transmitting includes “transferring funds on behalf of the
public by any and all means including but not limited to transfers within this country or to locations
abroad by wire, check, draft, facsimile, or courier.” This statute makes it a violation to conduct a
“money transmitting business” if the business is not registered as a money transmitting business with the
Secretary of the Treasury as required by a separate statute, Title 31, United States Code, Section 5330
and federal regulations pursuant to that statute.

19 * 59. The regulations specifically apply to foreign-based money transmitting businesses doing
20 substantial business in the United States. See C.F.R. §§ 1010.100(ff)(5), 1022.380(a)(2).

21 60. From in or about 2011, up to and including in or about May 2016, both dates being
22 approximate and inclusive, in the Northern District of California and elsewhere, the defendants,

BTC-e a/k/a CANTON BUSINESS CORPORATION, and
ALEXANDER VINNIK,

and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of a money transmitting business affecting interstate and foreign commerce, i.e. BTC-e, which (i) failed to comply with the money transmitting business

1 registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations
2 prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5) and 1022.380(a)(2);
3 and (ii) otherwise involved the transportation and transmission of funds known to the defendants to have
4 been derived from a criminal offense and intended to be used to promote and support unlawful activity.

5 All in violation of Title 18, United States Code, Sections 1960 & 2.

6 COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)
7

8 61. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein
9 as if set forth in full.

10 62. From in or about July 2011, through in or about January 2017, both dates being
11 approximate and inclusive, within the Northern District of California, and elsewhere, the defendants;

12 BTC-e a/k/a CANTON BUSINESS CORPORATION, and
13 ALEXANDER VINNIK,

14 and others known and unknown to the Grand Jury, willfully and knowingly did combine, conspire,
15 confederate, and agree together and with each other to knowingly conduct and attempt to conduct
16 financial transactions affecting interstate commerce and foreign commerce, which transactions involved
17 the proceeds of specified unlawful activity, that is, operation of an unregistered money transmitting
18 business in violation of Title 18, United States Code, Sections 1960; computer hacking and intrusions in
19 violation of Title 18, United States Code, Section 1030; identity theft in violation of Title 18, United
20 States Code, Section 1028; interstate transportation of stolen property in violation of Title 18, United
21 States Code, Section 2314; theft of government proceeds and extortion in violation of Title 18, United
22 States Code, Sections 641 and 1951; and narcotics trafficking in violation of Title 21, United States
23 Code, Section 841; with the intent to promote the carrying on of the specified unlawful activity, and that
24 while conducting and attempting to conduct such financial transactions, knew that the property involved
25 in the financial transactions represented the proceeds of some form of unlawful activity, in violation of
26 Title 18, United States Code, Section 1956(a)(1)(A)(i).

27 All in violation of Title 18, United States Code, Section 1956(h).
28

1 COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) Money
 2 Laundering)

3 On or about the dates described below, in the Northern District of California and elsewhere, the
 4 defendant,

5 ALEXANDER VINNIK,
 6 aided and abetted by others, known and unknown to the Grand Jury, did knowingly conduct and attempt
 7 to conduct the listed financial transactions affecting interstate and foreign commerce which involved the
 8 proceeds of a specified unlawful activity, that is accessing a computer in furtherance of fraud, in
 9 violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A), with the intent to promote
 10 the carrying on of said specified unlawful activity, and knowing that the transaction was designed in
 11 whole and in part to conceal and disguise the nature, location, source, ownership, and proceeds of said
 12 specified unlawful activity, and that while conducting and attempting to conduct such financial
 13 transaction, knew that the property involved in the financial transaction represented the proceeds of
 14 some form of unlawful activity.

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
THREE	01/23/2012	90 BTC	\$567.00	Transfer of BTC into Tradehill
FOUR	01/23/2012	83 BTC	\$522.07	Transfer of BTC into Tradehill
FIVE	01/23/2012	61 BTC	\$383.69	Transfer of BTC into Tradehill
SIX	01/24/2012	91 BTC	\$573.30	Transfer of BTC into Tradehill
SEVEN	01/24/2012	90 BTC	\$567.00	Transfer of BTC into Tradehill
EIGHT	01/24/2012	99 BTC	\$623.70	Transfer of BTC into Tradehill
NINE	01/24/2012	533 BTC	\$3,357.90	Transfer of BTC into Tradehill
TEN	01/24/2012	1900 BTC	\$11,970.00	Transfer of BTC into Tradehill
ELEVEN	01/24/2012	579 BTC	\$3,647.70	Transfer of BTC into Tradehill
TWELVE	01/24/2012	2 BTC	\$12.60	Transfer of BTC into Tradehill
THIRTEEN	01/27/2012	1000 BTC	\$5,290.00	Transfer of BTC into Tradehill
FOURTEEN	01/27/2012	1500 BTC	\$7,935.00	Transfer of BTC into Tradehill
FIFTEEN	02/01/2012	1000 BTC	\$5,820.00	Transfer of BTC into Tradehill
SIXTEEN	02/01/2012	1000 BTC	\$5,820.00	Transfer of BTC into Tradehill
SEVENTEEN	02/05/2012	3000 BTC	\$17,040.00	Transfer of BTC into Tradehill
EIGHTEEN	02/05/2012	500 BTC	\$2,840.00	Transfer of BTC into Tradehill
NINETEEN	02/12/2012	2000 BTC	\$11,200.00	Transfer of BTC into Tradehill

27 All in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i), (a)(1)(B)(i), and 2.
 28

1
2
3 COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 Engaging in Unlawful
4 Monetary Transactions)

5 On or about the dates described below, in the Northern District of California and elsewhere, the
6 defendant,

7 ALEXANDER VINNIK,

8 aided and abetted by others, known and unknown to the Grand Jury, did knowingly engage and attempt
9 to engage in the listed monetary transactions by through or to a financial institution affecting interstate
10 and foreign commerce in criminally derived property of a value greater than \$10,000, that is the
11 transactions listed below, such property having been derived from a specified unlawful activity, that is
12 accessing a computer in furtherance of fraud, in violation of Title 18, United States Code, Section
13 1030(a)(4) and (c)(3)(A).

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
TWENTY	02/05/2012	3000 BTC	\$17,040.00	Transfer of BTC into Tradehill
TWENTY-ONE	02/12/2012	2000 BTC	\$11,200.00	Transfer of BTC into Tradehill

17 All in violation of Title 18, United States Code, Sections 1957 and 2.

18
19 FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

20 63. All of the allegations contained in this Indictment are re-alleged and by this reference
21 fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18,
22 United States Code, Section 982(a)(1).

23 64. Upon a conviction for any of the offenses alleged in this Indictment, the defendants,

24 BTC-e a/k/a CANTON BUSINESS CORPORATION, and
25 ALEXANDER VINNIK,

26 shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal,
27 involved in those offenses or any property traceable to such offenses including but not limited to a
28 forfeiture money judgment.

If any of the aforementioned property, as a result of any act or omission of the defendants

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be divided without difficulty;

any and all interest the defendant has in other property shall be vested in the United States and
forfeited to the United States pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1).

All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal
Rules of Criminal Procedure.

DATED: 1/17/17

A TRUE BILL



FOREPERSON

BRIAN J. STRETCH
United States Attorney



BARBARA J. VALLIERE
Chief, Criminal Division

(Approved as to form: 
WILLIAM FRENTZEN
KATHRYN HAUN
Assistant U.S. Attorneys

**SEALED
BY COURT ORDER**

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CRIMINAL COVER SHEET

Instructions: Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.

CASE NAME: BTC-E aka/a Canton Business Corporation
USA v. and Alexander Vinnik

CASE NUMBER:
CR 16-00227 SI

Is This Case Under Seal? Yes No

Total Number of Defendants: 1 2-7 8 or more

Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326? Yes No

Venue (Per Crim. L.R. 18-1): SF OAK SJ

Is this a potential high-cost case? Yes No

Is any defendant charged with a death-penalty-eligible crime? Yes No

Is this a RICO Act gang case? Yes No

Assigned AUSA (Lead Attorney): William Frentzen Date Submitted: 01/17/2017

Comments:

1 BRIAN J. STRETCH (CABN 163973)
United States Attorney
2
3 BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division
4
5 WIL FRENTZEN (LABN 24421)
Assistant United States Attorney
6 450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
7 Telephone: (415) 436-6959
Fax: (415) 436-7234
William.Frentzen@usdoj.gov
8 Attorneys for the United States
9

2017 JAN 17 P 4:38
FILED
CLERK, U.S. DISTRICT COURT
NO. DIST. OF CA.

**SEALED
BY COURT ORDER**

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

13 UNITED STATES OF AMERICA,) CASE NO: CR 16-00227 SI
14 Plaintiff,)
15 v.) UNITED STATES' MOTION TO SEAL
16 BTC-E, A/K/A CANTON BUSINESS) SUPERSEDING INDICTMENT, ARREST
CORPORATION,) WARRANTS AND ~~PROPOSED~~ ORDER
17 and)
18 ALEXANDER VINNIK.)
19 Defendants.)
20
21
22
23
24
25
26
27
28

I hereby certify that the annexed
instrument is a true and correct copy
of the original on file in my office

ATTEST:

SUSAN Y SOONG
Clerk, U.S. District Court
Northern District of California

By *[Signature]* Deputy Clerk
Date *8/8/17*

MOTION TO SEAL

The United States hereby moves the Court for an order sealing this Motion and Order, Arrest Warrants and the Superseding Indictment. The government believes that if the defendants are made aware of these documents before they are arrested, that they may make efforts to avoid being arrested.

Date: January 17, 2017

Respectfully Submitted,

BRIAN J. STRETCH
United States Attorney

WILLIAM FRENTZEN
Assistant United States Attorney

[PROPOSED] ORDER

Based upon the foregoing request, the Court hereby **ORDERS** that this Motion and Order, Arrest Warrants and the Superseding Indictment shall be filed and kept under seal by the clerk of the Court until further order of the Court. The Court hereby further **ORDERS** that any representative of the United States Attorney's Office or the Internal Revenue Service, shall be allowed to obtain a copy of the Superseding Indictment without further order of the Court.

Dated: January 7, 2017

Sallie
HON. SALLIE KIM
UNITED STATES MAGISTRATE JUDGE

C

A

C

1 EXHIBIT C

12 **Statutes**

STATUTES

Count One:

Title 18, United States Code, Section 1960(a): Prohibition of Unlicensed Money Transmitting Businesses

(a) Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

(b) As used in this section

(1) the term “unlicensed money transmitting business” means a money transmitting business which affects interstate or foreign commerce in any manner or degree and—

(A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;

(2) the term “money transmitting” includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier; and

(3) the term “State” means any State of the United States, the District of Columbia, the Northern Mariana Islands, and any commonwealth, territory, or possession of the United States.

Count Two:

Title 18, United States Code, Section 1956(h): Laundering of Monetary Instruments

(a)

(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to

conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity

(A)

- (i) with the intent to promote the carrying on of specified unlawful activity; or
- (ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part—

- (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
- (ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than \$500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both. For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of specified unlawful activity if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.

(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States

(A) with the intent to promote the carrying on of specified unlawful activity; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

- (ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than \$500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both. For the purpose of the offense described in subparagraph (B), the defendant's knowledge may be established by proof that a law enforcement officer represented the matter specified in subparagraph (B) as true, and the defendant's subsequent statements or actions indicate that the defendant believed such representations to be true.

(3) Whoever, with the intent

- (A) to promote the carrying on of specified unlawful activity;
- (B) to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or
- (C) to avoid a transaction reporting requirement under State or Federal law,

conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. For purposes of this paragraph and paragraph (2), the term "represented" means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section.

(c) As used in this section

(1) the term "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity" means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7);

(2) the term "conducts" includes initiating, concluding, or participating in initiating, or concluding a transaction;

(3) the term "transaction" includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a

deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected;

(4) the term "financial transaction" means (A) a transaction which in any way or degree affects interstate or foreign commerce (i) involving the movement of funds by wire or other means or (ii) involving one or more monetary instruments, or (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5) the term "monetary instruments" means (i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;

(6) the term "financial institution" includes

(A) any financial institution, as defined in section 5312(a)(2) of title 31, United States Code, or the regulations promulgated thereunder; and

(B) any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101);

(7) the term "specified unlawful activity" means

(A) any act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31;

(D) an offense under ... section 641 (relating to public money, property, or records), ... section 1030 (relating to computer fraud and abuse) ...

(8) the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States; and

(9) the term "proceeds" means any property derived from or obtained or retained, directly or indirectly, through some form of unlawful activity, including the gross receipts of such activity.

- (f) There is extraterritorial jurisdiction over the conduct prohibited by this section if
- (1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and
 - (2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding \$10,000.
- (h) Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.
- (i) VENUE.
- (1) Except as provided in paragraph (2), a prosecution for an offense under this section or section 1957 may be brought in
 - (A) any district in which the financial or monetary transaction is conducted; or
 - (B) any district where a prosecution for the underlying specified unlawful activity could be brought, if the defendant participated in the transfer of the proceeds of the specified unlawful activity from that district to the district where the financial or monetary transaction is conducted.
 - (2) A prosecution for an attempt or conspiracy offense under this section or section 1957 may be brought in the district where venue would lie for the completed offense under paragraph (1), or in any other district where an act in furtherance of the attempt or conspiracy took place.
 - (3) For purposes of this section, a transfer of funds from 1 place to another, by wire or any other means, shall constitute a single, continuing transaction. Any person who conducts (as that term is defined in subsection (c)(2)) any portion of the transaction may be charged in any district in which the transaction takes place.

Title 18, United States Code, Section 1961: Definitions

As used in this chapter

- (1) "racketeering activity" means ... (B) any act which is indictable under any of the following provisions of title 18, United States Code: ... section 1028 (relating to fraud and related activity in connection with identification documents), ... section 1951 (relating to interference with commerce, robbery, or extortion) ... section 1960 (relating to illegal money transmitters), ... sections 2314 and 2315 (relating to interstate transportation of stolen property)

Counts Three through Nineteen:

Title 18, United States Code, Section 1956(a)(1): Laundering of Monetary Instruments

(see above)

Count Twenty through Twenty-One:

Title 18, United States Code, Section 1957: Unlawful Monetary Transactions

(a) Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b).

(b)

(1) Except as provided in paragraph (2), the punishment for an offense under this section is a fine under title 18, United States Code, or imprisonment for not more than ten years or both. If the offense involves a pre-retail medical product (as defined in section 670) the punishment for the offense shall be the same as the punishment for an offense under section 670 unless the punishment under this subsection is greater.

(2) The court may impose an alternate fine to that imposable under paragraph (1) of not more than twice the amount of the criminally derived property involved in the transaction.

(c) In a prosecution for an offense under this section, the Government is not required to prove the defendant knew that the offense from which the criminally derived property was derived was specified unlawful activity.

(d) The circumstances referred to in subsection (a) are

(1) that the offense under this section takes place in the United States or in the special maritime and territorial jurisdiction of the United States; or
(2) that the offense under this section takes place outside the United States and such special jurisdiction, but the defendant is a United States person (as defined in section 3077 of this title, but excluding the class described in paragraph (2)(D) of such section).

(f) As used in this section

(1) the term "monetary transaction" means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary

instrument (as defined in section 1956(c)(5) of this title) by, through, or to a financial institution (as defined in section 1956 of this title), including any transaction that would be a financial transaction under section 1956(c)(4)(B) of this title, but such term does not include any transaction necessary to preserve a person's right to representation as guaranteed by the sixth amendment to the Constitution;

- (2) the term "criminally derived property" means any property constituting, or derived from, proceeds obtained from a criminal offense; and
- (3) the terms "specified unlawful activity" and "proceeds" shall have the meaning given those terms in section 1956 of this title.

Forfeiture:

Title 18, United States Code, Section 982: Criminal Forfeiture

(a)

(1) The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

(b)

(1) The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(2) The substitution of assets provisions of subsection 413(p) shall not be used to order a defendant to forfeit assets in place of the actual property laundered where such defendant acted merely as an intermediary who handled but did not retain the property in the course of the money laundering offense unless the defendant, in committing the offense or offenses giving rise to the forfeiture, conducted three or more separate transactions involving a total of \$100,000 or more in any twelve month period.

Title 18, United States Code, Section 981: Civil Forfeiture

(a)

(1) The following property is subject to forfeiture to the United States:

(A) Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.

(B) Any property, real or personal, within the jurisdiction of the United States, constituting, derived from, or traceable to, any proceeds obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense

(i) involves trafficking in nuclear, chemical, biological, or radiological weapons technology or material, or the manufacture, importation, sale, or distribution of a controlled substance (as that term is defined for purposes of the Controlled Substances Act), or any other conduct described in section 1956(c)(7)(B);

(ii) would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding 1 year; and

(iii) would be punishable under the laws of the United States by imprisonment for a term exceeding 1 year, if the act or activity constituting the offense had occurred within the jurisdiction of the United States.

(C) Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section 215, 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 656, 657, 670, 842, 844, 1005, 1006, 1007, 1014, 1028, 1029, 1030, 1032, or 1344 of this title or any offense constituting “specified unlawful activity” (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

Title 21, United States Code, Section 853: Criminal Forfeiture

(a) Property subject to criminal forfeiture: Any person convicted of a violation of this subchapter or subchapter II punishable by imprisonment for more than one year shall forfeit to the United States, irrespective of any provision of State law—

(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation;

(2) any of the person’s property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation; and

(3) in the case of a person convicted of engaging in a continuing criminal enterprise in violation of section 848 of this title, the person shall forfeit, in addition to any property described in paragraph (1) or (2), any of his interest in,

claims against, and property or contractual rights affording a source of control over, the continuing criminal enterprise.

The court, in imposing sentence on such person, shall order, in addition to any other sentence imposed pursuant to this subchapter or subchapter II, that the person forfeit to the United States all property described in this subsection. In lieu of a fine otherwise authorized by this part, a defendant who derives profits or other proceeds from an offense may be fined not more than twice the gross profits or other proceeds.

(p) Forfeiture of substitute property

(1) In general: Paragraph (2) of this subsection shall apply, if any property described in subsection (a), as a result of any act or omission of the defendant

- (A) cannot be located upon the exercise of due diligence;
- (B) has been transferred or sold to, or deposited with, a third party;
- (C) has been placed beyond the jurisdiction of the court;
- (D) has been substantially diminished in value; or
- (E) has been commingled with other property which cannot be divided without difficulty.

(2) Substitute property: In any case described in any of subparagraphs (A) through (E) of paragraph (1), the court shall order the forfeiture of any other property of the defendant, up to the value of any property described in subparagraphs (A) through (E) of paragraph (1), as applicable.

Federal Rule of Criminal Procedure 32.2(a)

(a) NOTICE TO THE DEFENDANT. A court must not enter a judgment of forfeiture in a criminal proceeding unless the indictment or information contains notice to the defendant that the government will seek the forfeiture of property as part of any sentence in accordance with the applicable statute. The notice should not be designated as a count of the indictment or information. The indictment or information need not identify the property subject to forfeiture or specify the amount of any forfeiture money judgment that the government seeks.

Aiding and Abetting:

Title 18, United States Code, Section 2: Principals

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

Statute of Limitations:

Title 18, United States Code, Section 3282: Offenses Not Capital

(a) **In General.** Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

Supplemental Statutes:

Title 31, United States Code, Section 5330: Registration of Money Transmitting Businesses

(a) Registration With Secretary of the Treasury Required.

(1) In general. Any person who owns or controls a money transmitting business shall register the business (whether or not the business is licensed as a money transmitting business in any State) with the Secretary of the Treasury not later than the end of the 180-day period beginning on the later of

(A) the date of enactment of the Money Laundering Suppression Act of 1994; or

(B) the date on which the business is established.

(2) Form and manner of registration. Subject to the requirements of subsection (b), the Secretary of the Treasury shall prescribe, by regulation, the form and manner for registering a money transmitting business pursuant to paragraph (1).

(3) Businesses remain subject to state law. This section shall not be construed as superseding any requirement of State law relating to money transmitting businesses operating in such State.

(4) False and incomplete information. The filing of false or materially incomplete information in connection with the registration of a money transmitting business shall be considered as a failure to comply with the requirements of this subchapter.

(b) Contents of Registration. The registration of a money transmitting business under subsection (a) shall include the following information:

- (1) The name and location of the business.
 - (2) The name and address of each person who
 - (A) owns or controls the business;
 - (B) is a director or officer of the business; or
 - (C) otherwise participates in the conduct of the affairs of the business.
 - (3) The name and address of any depository institution at which the business maintains a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act).
 - (4) An estimate of the volume of business in the coming year (which shall be reported annually to the Secretary).
 - (5) Such other information as the Secretary of the Treasury may require.
- (c) Agents of Money Transmitting Businesses.
- (1) Maintenance of lists of agents of money transmitting businesses. Pursuant to regulations which the Secretary of the Treasury shall prescribe, each money transmitting business shall
 - (A) maintain a list containing the names and addresses of all persons authorized to act as an agent for such business in connection with activities described in subsection (d)(1)(A) and such other information about such agents as the Secretary may require; and
 - (B) make the list and other information available on request to any appropriate law enforcement agency.
 - (2) Treatment of agent as money transmitting business. The Secretary of the Treasury shall prescribe regulations establishing, on the basis of such criteria as the Secretary determines to be appropriate, a threshold point for treating an agent of a money transmitting business as a money transmitting business for purposes of this section.
- (d) Definitions. For purposes of this section, the following definitions shall apply:
- (1) Money transmitting business. The term "money transmitting business" means any business other than the United States Postal Service which
 - (A) provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks,

and other similar instruments or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;

(B) is required to file reports under section 5313; and

(C) is not a depository institution (as defined in section 5313(g)).

(2) Money transmitting service. The term “money transmitting service” includes accepting currency or funds denominated in the currency of any country and transmitting the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal reserve bank or other facility of the Board of Governors of the Federal Reserve System, or an electronic funds transfer network.

FinCEN Guidance:

FIN-2013-G001: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

The Financial Crimes Enforcement Network (“FinCEN”) is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act (“BSA”) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.¹ Such persons are referred to in this guidance as “users,” “administrators,” and “exchangers,” all as defined below.² A user of virtual currency is *not* an MSB under FinCEN’s regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger *is* an MSB under FinCEN’s regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN’s regulations.

¹ FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. See Treasury Order 180-01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.

² FinCEN’s regulations define “person” as “an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.” 31 CFR § 1010.100(mm).

Currency vs. Virtual Currency

FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."³ In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

Background

On July 21, 2011, FinCEN published a Final Rule amending definitions and other regulations relating to money services businesses ("MSBs").⁴ Among other things, the MSB Rule amends the definitions of dealers in foreign exchange (formerly referred to as "currency dealers and exchangers") and money transmitters. On July 29, 2011, FinCEN published a Final Rule on Definitions and Other Regulations Relating to Prepaid Access (the "Prepaid Access Rule").⁵ This guidance explains the regulatory treatment under these definitions of persons engaged in virtual currency transactions.

Definitions of User, Exchanger, and Administrator

This guidance refers to the participants in generic virtual currency arrangements, using the terms "user," "exchanger," and "administrator."⁶ A *user* is a person that obtains virtual currency to purchase goods or services.⁷ An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

³ 31 CFR § 1010.100(m).

⁴ *Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011) (the "MSB Rule"). This defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States." 31 CFR § 1010.100(ff).

⁵ *Final Rule – Definitions and Other Regulations Relating to Prepaid Access*, 76 FR 45403 (July 29, 2011)

⁶ These terms are used for the exclusive purpose of this regulatory guidance. Depending on the type and combination of a person's activities, one person may be acting in more than one of these capacities.

⁷ How a person engages in "obtaining" a virtual currency may be described using any number of other terms, such as "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing," depending on the details of the specific virtual currency model involved. For purposes of this guidance, the label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the BSA of the process or of the person engaging in the process.

Users of Virtual Currency

A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is *not* an MSB under FinCEN's regulations.⁸ Such activity, in and of itself, does not fit within the definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.⁹

Administrators and Exchangers of Virtual Currency

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.¹⁰ FinCEN's regulations define the term "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."¹¹

The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.¹² FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and de-centralized convertible virtual currencies.

a. E-Currencies and E-Precious Metals

⁸ As noted above, this should not be interpreted as a statement about the extent to which the user's activities comport with other federal or state statutes, rules, regulations, or orders. For example, the activity may still be subject to abuse in the form of trade-based money laundering or terrorist financing. The activity may follow the same patterns of behavior observed in the "real" economy with respect to the purchase of "real" goods and services, such as systematic over- or under-invoicing or inflated transaction fees or commissions.

⁹ 31 CFR § 1010.100(ff)(1-7).

¹⁰ FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)-(F).

¹¹ 31 CFR § 1010.100(ff)(5)(i)(A).

¹² Ibid.

The first type of activity involves electronic trading in e-currencies or e-precious metals.¹³ In 2008, FinCEN issued guidance stating that as long as a broker or dealer in real currency or other commodities accepts and transmits funds solely for the purpose of effecting a *bona fide* purchase or sale of the real currency or other commodities for or with a customer, such person is not acting as a money transmitter under the regulations.¹⁴

However, if the broker or dealer transfers funds between a customer and a third party that is not part of the currency or commodity transaction, such transmission of funds is no longer a fundamental element of the actual transaction necessary to execute the contract for the purchase or sale of the currency or the other commodity. This scenario is, therefore, money transmission.¹⁵ Examples include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer's account; (2) the transfer of value from a customer's currency or commodity position to the account of another customer; or (3) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party. Since the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies, the same rules apply to brokers and dealers of e-currency and e-precious metals.

b. Centralized Virtual Currencies

The second type of activity involves a convertible virtual currency that has a centralized repository. The administrator of that repository will be a money transmitter to the extent that it allows transfers of value between persons or from one location to another. This conclusion applies, whether the value is denominated in a real currency or a convertible virtual currency. In addition, any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on

¹³ Typically, this involves the broker or dealer electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency. However, the same conclusions would apply in the case of the broker or dealer issuing paper ownership certificates or manifesting customer ownership or control of real currencies or commodities in an account statement or any other form. These conclusions would also apply in the case of a broker or dealer in commodities other than real currencies or precious metals. A broker or dealer of e-currencies or e-precious metals that engages in money transmission could be either an administrator or exchanger depending on its business model.

¹⁴ *Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities*, FIN-2008-G008, Sept. 10, 2008. The guidance also notes that the definition of money transmitter excludes any person, such as a futures commission merchant, that is "registered with, and regulated or examined by...the Commodity Futures Trading Commission."

¹⁵ In 2011, FinCEN amended the definition of money transmitter. The 2008 guidance, however, was primarily concerned with the core elements of the definition – accepting and transmitting currency or value – and the exemption for acceptance and transmission integral to another transaction not involving money transmission. The 2011 amendments have not materially changed these aspects of the definition.

behalf of others, including transfers intended to pay a third party for virtual goods and services, is also a money transmitter.

FinCEN understands that the exchanger's activities may take one of two forms. The first form involves an exchanger (acting as a "seller" of the convertible virtual currency) that accepts real currency or its equivalent from a user (the "purchaser") and transmits the value of that real currency to fund the user's convertible virtual currency account with the administrator. Under FinCEN's regulations, sending "value that substitutes for currency" to another person or to another location constitutes money transmission, unless a limitation to or exemption from the definition applies.¹⁶ This circumstance constitutes transmission *to another location*, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator. It might be argued that the exchanger is entitled to the exemption from the definition of "money transmitter" for persons involved in the sale of goods or the provision of services. Under such an argument, one might assert that the exchanger is merely providing the service of connecting the user to the administrator and that the transmission of value is integral to this service. However, this exemption does not apply when the only services being provided are money transmission services.¹⁷

The second form involves a *de facto* sale of convertible virtual currency that is not completely transparent. The exchanger accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the exchanger's own convertible virtual currency held with the administrator of the repository. The exchanger then transmits that internally credited value to third parties at the user's direction. This constitutes transmission *to another person*, namely each third party to which transmissions are made at the user's direction. To the extent that the convertible virtual currency is generally understood as a substitute for real currencies, transmitting the convertible virtual currency at the direction and for the benefit of the user constitutes money transmission on the part of the exchanger.

c. De-Centralized Virtual Currencies

A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort.

A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to

¹⁶ See footnote 11 and adjacent text.

¹⁷ 31 CFR § 1010.100(ff)(5)(ii)(F).

another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.

Providers and Sellers of Prepaid Access

A person's acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies.¹⁸

Dealers in Foreign Exchange

A person must exchange the currency of two or more countries to be considered a dealer in foreign exchange.¹⁹ Virtual currency does not meet the criteria to be considered "currency" under the BSA, because it is not legal tender. Therefore, a person who accepts real currency in exchange for virtual currency, or *vice versa*, is not a dealer in foreign exchange under FinCEN's regulations.

¹⁸ This is true even if the person holds the value accepted for a period of time before transmitting some or all of that value at the direction of the person from whom the value was originally accepted. FinCEN's regulations define "prepaid access" as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number." 31 CFR § 1010.100(ww). Thus, "prepaid access" under FinCEN's regulations is limited to "access to funds or the value of funds." If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency." 31 CFR § 1010.100(ff)(5)(i).

¹⁹ FinCEN defines a "dealer in foreign exchange" as a "person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than \$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery." 31 CFR § 1010.100(ff)(1).

D

EXHIBIT D

Affidavit of SA Delaney

1 BRIAN J. STRETCH (CABN 163973)
2 United States Attorney

3 BARBARA VALLIERE (CABN 147374)
4 Chief, Criminal Division

5 WILLIAM FRENTZEN (LABN 24421)
6 Assistant United States Attorney

7 450 Golden Gate Avenue, Box 36055
8 San Francisco, California 94102-3495
9 Telephone: (415) 436-6959
10 Fax: (415) 436-7234
11 William.Frentzen@usdoj.gov

12 Attorneys for United States of America

13
14 UNITED STATES DISTRICT COURT
15 FOR THE NORTHERN DISTRICT OF CALIFORNIA
16
17 SAN FRANCISCO DIVISION

18 UNITED STATES OF AMERICA,

19) No. CR 16-00227 RS

20 Plaintiff,

21) AFFIDAVIT OF HOMELAND SECURITY
22 v.) INVESTIGATIONS SPECIAL AGENT
23 BTC-E, and) MICHAEL DELANEY IN SUPPORT OF
24 ALEXANDER VINNIK,) REQUEST FOR EXTRADITION OF
25) ALEXANDER VINNIK

26 Defendants.

27 I, Michael Delaney, being duly sworn, depose and state:

28 1. I am a citizen of the United States of America, and a resident of the state of California.

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland

2. Security Investigations (HSI) and have been so employed since February 2012. I am assigned to HSI's
3 San Francisco field office and investigate financial crime and cybercrime. I have been a law
4

enforcement officer for over 30 years, including eight years as a Berkeley, CA police officer; 15 years as a Special Agent with the U.S. Drug Enforcement Administration (DEA); and five as a Special Agent with NASA's Office of Inspector General. I am a graduate of the DEA Academy in Quantico, Virginia and HSI's Special Agent training program at the Federal Law Enforcement Training Center in Georgia. This training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and execution of search warrants. Since graduating, I have received further training in Federal and California laws and investigative techniques relating to criminal enterprises and financial crime. I have also given specialized instruction concerning money laundering to local, state, federal, and foreign law enforcement as well as private sector entities.

3. My duties have included participating in the ongoing investigation of Alexander VINNIK (“VINNIK”), who has been indicted in the criminal case captioned United States v. BTC-E and Alexander VINNIK, Case Number 16-CR-227 (RS) (Northern District of California). As one of the investigators, I am familiar with the evidence in the case.

BACKGROUND

4. The investigation has revealed that, from 2011 through the present, VINNIK operated an unlicensed money transmitting business, conspired to launder money, and did launder money in violation of United States law.

5. VINNIK is charged in an indictment dated January 17, 2017, with the following offenses:

6. Count One: Illegally operating an unlicensed money transmitting business, in violation of Title 18, United States Code, Section 1960. By operating a money transmitting business that handled money from the United States and did not register with the Financial Crimes Enforcement Network (“FinCEN”), BTC-e and VINKI avoided controls that they would have to implement to prevent the laundering of illegal proceeds through the digital currency exchange BTC-e.

7. Count Two: Illegally agreeing and conspiring to launder money in violation of Title 18, United States Code, Section 1956(h). By operating BTC-e without any safeguards for money launderers, VINNIK and his fellow managers and conspirators knew and agreed that they were creating a platform for money laundering throughout the world, including in the United States.

8. Counts Three through Nineteen: Money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i) and (a)(1)(B)(i). VINNIK used BTC-e and a digital currency exchange called Tradehill to launder digital currency stolen through illegal computer access by fraud and conducted financial transactions in order to disguise and conceal the ownership and source of the proceeds.

9. Counts Twenty and Twenty-One: Money laundering, in violation of Title 18, United States Code, Section 1957. VINNIK used BTC-e and a digital currency exchange called Tradehill to launder digital currency stolen through illegal computer access by fraud and conducted monetary transactions in excess of \$10,000 with the proceeds.

10. I have reviewed reports of interviews, reviewed statements of witnesses in this case, interviewed witnesses personally, viewed the results from online undercover operations, reviewed results from search warrants including the imaging of the servers of BTC-e, reviewed translated emails, reviewed bank records, reviewed hotel and travel records, and reviewed and analyzed pen register data. I have also consulted with experts in the areas of computer forensics and tracing digital currency regarding VINNIK and the operation of BTC-e.

SUMMARY OF THE EVIDENCE

Witness A

REDACTED

¹ Throughout this affidavit, I made reference to Witnesses by letters rather than names and are referred to in the masculine despite actual gender. The identities of all witnesses will be made known prior to trial.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

REDACTED

Witness B

13. Witness B is an Internal Revenue Service (IRS) Criminal Investigations Special Agent and one of the primary investigators of BTC-e and VINNIK. As a result of the information that BTC-e was a popular exchange for illegal actors who wished to conceal true identities from law enforcement, Witness B began communicating with BTC-e by email, posing as a potential customer.

14. Witness B had occasion to deal with BTC-e in a limited undercover capacity. Using an undercover email account, Witness B communicated with BTC-e. Witness B registered an account with BTC-e by providing no identifying information. Witness B was able to contact BTC-e support via its Internet interface, which generated a numbered “support ticket.” The BTC-e support system software tracked individual customer communications within BTC-e’s platform. Witness B asked BTC-e whether they accepted wire transfers to and from U.S. banks. On February 23, 2016, BTC-E support responded that they did. Witness B did not need anything other than an email address to open the BTC-e account, and, accordingly, no identity was ever verified. Like Witness A, Witness B has information as to how BTC-e works and its fee structure.

15. Witness B has reviewed documents obtained from a variety of sources including a court-authorized search of the BTC-e databases in December 2015 and January 2016, emails, and

1 search warrants that demonstrate that VINNIK is the person who controls certain emails and accounts
 2 that are intrinsic to the operation and administration of BTC-e. In other words, Witness B knows the
 3 various pieces of evidence that conclusively connect VINNIK as the operator and manager of BTC-e.

4 16. For example, a key email account controlling BTC-e operations has been identified as
 5 wmewme@gmail.com (the “wme” address). This email address is connected directly to VINNIK
 6 because (1) it connects to “cookies”² from the same device as accounts known to belong to VINNIK’s
 7 wife, Alexandra Shevchenko,³ meaning that the user of “wme” address uses the same computer as
 8 VINNIK’s wife and (2) VINNIK has used “wme” address to book vacations for himself and his family.

9 17. From Witness B’s review of the evidence, he has learned that VINNIK has made efforts
 10 to conceal his true identity by using aliases, including Stanislav Golovanov. VINNIK has tried to use
 11 Golovanov as a false identity when conducting BTC-e business; however, the true identity of
 12 Golovanov in these instances is actually VINNIK. For example, on several occasions, the “wme”
 13 address has been used to send invoices out on behalf of BTC-e. As pointed out above, VINNIK
 14 controls the “wme” address, but the invoices sent out purport to have been signed by Golovanov on
 15 behalf of BTC-e. Additionally, Witness B has located instances where emails purportedly belonging to
 16 Golovanov were auto-forwarded to addresses held by VINNIK. For example, in managing BTC-e
 17 business, golovanov.stas@gmail.com and stanislav.golovanov@aol.com were auto-forwarded to the
 18 “wme” address that VINNIK controlled. Obviously, if Golovanov were a real administrator at BTC-e,
 19 he would not have his emails auto-forwarded to VINNIK.

20 18. Similarly, Witness B has analyzed another VINNIK email used to conduct business on
 21 behalf of BTC-e, vasily.sidorov.msk@gmail.com (the “Sidorov” address). Vasily Sidorov is another
 22

23 ² An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie)
 24 is a small piece of data sent from a website and stored on the user’s computer by the user’s web browser
 while the user is browsing. Cookies can be used by websites to track browsing by computers.

25 ³ For ease of discussion in this document I am referring to Alexandra Shevchenko as the “wife”
 26 of VINNIK. It is actually unknown if Shevchenko and VINNIK are legally married. What is known
 27 from travel records and from Shevchenko’s Instagram account is that Shevchenko and VINNIK live
 together with a relatively lavish lifestyle for Russian citizens (luxury apartment in Moscow and a
 weekend home in suburban Moscow valued at approximately \$3 million U.S. dollars), take luxury
 28 vacations together to locations such as Greece and Dubai, socialize with friends together, spend
 holidays together, and appear to be raising two children together. From this evidence, it is clear that
 VINNIK and Shevchenko are either married or in a relationship and that they are living together.

1 alias used by VINNIK to try to separate himself from the operation of BTC-e. Similar to the “wme”
2 address, the “Sidorov” address is known to be used by VINNIK due to links by cookies to the known
3 accounts of VINNIK’s wife, Alexandra Shevchenko. In one instance, VINNIK combined two of his
4 aliases to conduct BTC-e business by using the “Sidorov” address to open an online account in the
5 name of “Stanislav Golovanov.”

6 19. Witness B also analyzed another account that was used by VINNIK,
7 prepaidphonecards@gmail.com (the “prepaid” address) [for a description of the evidence linking
8 VINNIK to the “prepaid” address, refer to Witness F, below] and determined that VINNIK used the
9 address to switch a BTC-e account with an advertising company from a Golovanov-named email
10 address to the “prepaid” address.

11 20. From review of all of these accounts, Witness B has determined that Golovanov and
12 Sidorov are aliases for VINNIK that VINNIK often used to try to separate VINNIK’s true identity from
13 connection to operation of BTC-e. However, VINNIK has left forensic evidence to connect him
14 directly to the operation of BTC-e.

15 21. Witness B is familiar with money laundering techniques and the use of aliases to
16 separate true owners and managers from the laundering of proceeds. These techniques reflect an
17 awareness of those conducting the transactions that the proceeds are illegal and tend to demonstrate a
18 consciousness of guilt. In other words, if VINNIK believed that he were conducting a legitimate
19 money transmitting business, or digital currency exchange, then he would have no reason to take
20 elaborate steps to try to hide his true identity through aliases.

21 **Witness C**

22 22. Witness C is an undercover Internal Revenue Service Criminal Investigations Special
23 Agent (“Undercover Agent 1”), who posed as a potential customer and communicated with BTC-e by
24 email in an undercover capacity. Using an undercover account, Undercover Agent 1 communicated
25 with BTC-e. Undercover Agent 1 registered a BTC-e account providing no identifying information and
26 was able to contact BTC-e support via a support ticket like Witness B did.

27 23. Beginning on July 6, 2016, Undercover Agent 1 emailed BTC-e and said he was new to
28 the BTC-e website. Undercover Agent 1 asked to redeem bitcoins derived from AlphaBay a notorious

1 dark web site for illegal commodities such as narcotics and identification fraud.⁴ Undercover Agent 1
2 told BTC-e he had about \$5,000 in bitcoin that he wanted to sell on a regular basis. BTC-e replied again
3 that Undercover Agent 1 could "do this in any convenient time." Undercover Agent 1 told BTC-e he
4 was worried that his account would get "frozen" if he deposited and sold bitcoin obtained from
5 AlphaBay.

6 24. Undercover Agent 1 told BTC-e he had "a problem" redeeming bitcoin from an
7 American virtual currency exchange (that is AML/KYC-complaint) because it didn't want customers
8 with bitcoin it suspected was from heroin sales. BTC-e responded again that Undercover agent 1 could
9 "do this in any convenient time." Undercover Agent 1 then asked if he could transfer funds from his
10 bitcoin sales to his United States bank account, because he was concerned about "problems" with his
11 bank. BTC-e replied "No, we do not send bank transfers to US banks."

12 **Witness D**

13 25. Witness D is also an undercover Internal Revenue Service Special Agent ("Undercover
14 Agent 2"). Undercover Agent 2 sent BTC-e a series of communications from the Northern District of
15 California during 2017 to determine whether BTC-e would conduct monetary and financial transactions
16 with overtly criminal proceeds.

17 26. On May 19, 2017, Undercover Agent 2 communicated with BTC-e by asking if he could
18 "cash out bitcoin from AlphaBay" if he was located in San Francisco, California. In response, BTC-e
19 support said they do not accept that "payment system" but then informed Undercover Agent 2 how to
20 make a deposit into a BTC-e account.

21 27. Following that initial communication, Undercover Agent 2 persisted and asked if BTC-e
22 would reject a payment from an AlphaBay wallet because Undercover Agent 2 stated that other
23 [compliant] digital currency exchanges had done so. Undercover Agent 2 also asked if it mattered that
24 he was in California. On May 21, 2017, BTC-e support responded that it did "not matter which purse
25 you use."

26
27
28 ⁴ AlphaBay was recently shut down by international law enforcement for operating an illegal
marketplace.

1 28. On May 22, 2017, Undercover Agent 2 asked again if it would matter to BTC-e that
 2 Undercover Agent 2 was in California, and if Undercover Agent 2 could use Citibank. BTC-e support
 3 claimed in a response that they do not deal with US citizens or US banks, but the evidence is that BTC-
 4 e has and does regularly deal with US citizens and US banks. In fact, because BTC-e asks virtually no
 5 identifying information, it willfully avoids knowing the nationalities of its users.

6 29. On May 24, 2017, Undercover Agent 2 after already indicating his digital currency
 7 came from AlphaBay and that he was in the US reached out again to ask BTC-e “I just want to
 8 confirm that if I deposit and sell Bitcoin I earned on AlphaBay that my account is not going to get
 9 frozen or scrutinized. I previously had a problem redeeming Bitcoin using another exchange that
 10 determined that I had earned the bitcoin from **illegal drug sales**. I plan to sell bitcoin on BTC-E
 11 regularly and want to make sure I am not going to have that sort of scrutiny.” (Emphasis added). The
 12 response from BTC-e support to this obviously criminal attempt to use the site was only that BTC-e did
 13 not support generated transactions from “pools,” but that “[y]ou should not encounter other problems
 14 when using our service.”

15 30. Despite Undercover Agent 2 informing BTC-e that he was a US citizen using US banks
 16 to move funds from an illegal dark web site and that he had proceeds from illegal drug sales, on June
 17 12, 2017, Undercover Agent 2 moved 4.21708793 bitcoin into an account at BTC-e. BTC-e accepted
 18 the bitcoin. On June 14 and 15, 2017, Undercover Agent 2 withdrew the funds through a US account at
 19 PayPal despite BTC-e support’s claims that it did not deal with US banks or US citizens.

20 **Witness E**

21 31. Witness E works for the U.S. Treasury Department and the Financial Crimes
 22 Enforcement Network (“FinCEN”). Witness E is aware from records checks that BTC-e has never
 23 been registered with FinCEN as a money transmitting business. Witness E can also establish from
 24 records checks that BTC e has never filed a Suspicious Activity Report.⁵ Despite the countless
 25 instances of criminal uses of BTC-e that are indicative of if not blatantly obvious instances of

27 28 5 Suspicious Activity Reports are filed by US financial institutions with FinCEN to report
 financial activity and transactions noted to be suspicious or criminal in nature, typically involving
 money laundering or fraud. US law enforcement or banking regulators regularly use these reports to
 investigate financial crime.

1 laundering criminal proceeds that should have triggered a Suspicious Activity Report. BTC-e's method
 2 of business would have precluded BTC-e from registering with FinCEN because BTC-e did not have
 3 the proper procedures in place to operate as a legitimate business.

4 **Witness F**

5 32. As one of the primary investigating agents for this case, I am "Witness F." I've reviewed
 6 extensive records and documents from all sources in connection with this investigation. My
 7 investigation has confirmed that BTC-e was used to launder criminal funds derived from a series of
 8 computer intrusions and resulting thefts, including thefts from the Japan-based Mt. Gox digital currency
 9 exchange. Analysis of blockchain data⁶ and review of the BTC-e server data show a sizable portion of
 10 the stolen Mt. Gox bitcoin, totaling over 300,000 bitcoin (today worth approximately \$831 million US
 11 dollars) went into four BTC-e accounts controlled, owned, and operated by VINNIK. One of these
 12 accounts is the WME BTC-e account. The WME BTC-e account was directly linked to BTC-e
 13 administrative accounts, to which only BTC-e administrators and/or operators would have access. The
 14 investigation has revealed that VINNIK historically has used the "WME" moniker and that he exercised
 15 control over BTC-e's "WME" account.

16 33. The investigation revealed that portions of the stolen Mt. Gox bitcoin also were
 17 laundered through (a) the Tradehill Exchange in San Francisco, CA and (b) back into a second Mt. Gox
 18 account (hereinafter the "WME Mt. Gox account"). Investigation shows both the WME Mt. Gox
 19 account and the Tradehill account that received the stolen Mt. Gox bitcoin were controlled by a user
 20 known as "WME," who also controlled the BTC-e "**WME**" account.

21 34. The WME Mt. Gox account was used to launder 38,261 of the stolen Mt. Gox bitcoin
 22 (today worth approximately \$106 million US dollars). The account was created using the email address
 23 wmewme@gmail.com, and was verified with a passport of "Visiliy Siderov" sent from the WME
 24 Gmail account. By this time, VINNIK was using Sidorov as an alias. Vinnik also used the e-mail
 25

26
 27 ⁶ All bitcoin transactions are recorded on what is known as the Blockchain, an online distributed
 28 public ledger that tracks all incoming and outgoing bitcoin transactions and that updates approximately
 six times per hour. The Blockchain records every bitcoin address that has ever received a bitcoin and
 maintains records of every transaction for each bitcoin address.

1 address vasiliy.sidorov.msk@gmail.com to control one of the main BTC-e accounts, called the
 2 **vannnedam** account.

3 35. In addition to the money moved through the WME Mt. Gox account, 191,004 of the
 4 stolen Mt. Gox bitcoin (today worth approximately \$529 million) was also laundered through the
 5 Tradehill virtual currency exchange. The funds were associated with a customer known to Tradehill as
 6 “WME.” The WME customer corresponded with Tradehill using the email address
 7 wmewme@gmail.com, controlled by VINNIK. In one email from “WME,” VINNIK sent Tradehill a
 8 copy of his true Russian passport, as well as documentation naming VINNIK as director of the
 9 ALTVIGE CORPORATION.

10 36. Tradehill exchanged a portion of the stolen Mt. Gox bitcoin for US Dollars, which were
 11 transferred out of Tradehill’s Citibank account. I examined Citibank records that showed withdrawals
 12 in US dollars from Tradehill to an account at a bank in Cyprus. This Cypriot account was held in the
 13 name of the ALTVIGE CORPORATION, addressed in Belize City, Belize yet formed as a corporation
 14 in the Seychelles using prepaidphonecards@gmail.com. From training and experience, I am aware that
 15 that Belize bank accounts are widely used in Russia for foreign funds transfer, and the Seychelles is a
 16 known money laundering haven.

17 37. The investigation of VINNIK conducted by me and my colleagues determined VINNIK
 18 regularly used prepaidphonecards@gmail.com (the “prepaid” address) to launder money. Through
 19 publicly available sources, the investigative team found that VINNIK advertised three Apple computers
 20 and an iPhone for sale online in Russia over the past several years. His online listings were specific
 21 enough to read serial numbers and other identifying details of these devices. Agents served Apple
 22 Computer Inc. with a Grand Jury subpoena for customer information related to these devices.

23 38. Subsequently, Apple informed the investigative team that two of these computers and
 24 the iPhone were registered between 2010 and 2015 using the “prepaid” Gmail address under the name
 25 of Vera Sokolov (“Alex Sokol” is yet another one of VINNIK’s aliases) at a fictitious Russian address.
 26 The devices were also paired with other Apple services, such as iTunes, accessed by the “prepaid”
 27 address. The “prepaid” address was used on at least three of the devices linked to VINNIK, including
 28 an iPhone, from October to December 2015. One of VINNIK’s Macbooks was registered using his

1 “WME” Gmail address under the name Vera VINNIK, then linked to the “prepaid” address. However,
 2 both accounts were accessed from the same Russian IP address.

3 39. Since June 2016, Google Inc. provided data for VINNIK’s Gmail accounts
 4 wmewme@gmail.com, [vasiliy.sidorov.msk@gmail.com](mailto:vasily.sidorov.msk@gmail.com), and prepaidphonecards@gmail.com pursuant
 5 to Pen Register and Trap and Trace Orders authorized by US Judges. My review of the header data in
 6 several thousand of VINNIK’s emails indicates he continuously accessed his Gmail accounts from
 7 several common IP addresses – namely, an IP address with a Dutch proxy server⁷ that masked his true
 8 location and another IP address that resolved to Russia. I reviewed records from a virtual currency
 9 exchange that documented that VINNIK in 2016 used his true name, address, and passport information
 10 to establish two exchange accounts, one in his true name, and the other for a business named NANO
 11 ABC that received millions of dollars in its bank accounts, both created and accessed from the same
 12 Dutch proxy or Russian IP address.

13 40. When VINNIK arrived in Greece, the Pen Register and Trap and Trace analysis showed
 14 that he still used the Dutch proxy IP despite being in Greece, with one notable exception – on July 23,
 15 2017, despite VINNIK’s precaution using the proxy, he accessed his wmewme@gmail.com account
 16 from the same Greek IP address used to access his wife’s Instagram account earlier that day. While
 17 VINNIK was in Greece, he received emails from the server host managing BTC-e’s servers at a secure
 18 facility in New Jersey. Also, VINNIK sent emails to Russian financial operators such as MoneyPolo
 19 used to mule fiat currency in and out of BTC-e, and private Russian wealth management firms. Thus,
 20 VINNIK was managing BTC-e’s operations while vacationing in Greece.

21 41. I am familiar with money laundering techniques and use of aliases and shell companies
 22 to separate true owners and their accounts while laundering proceeds. These techniques reflect the
 23 knowledge of those conducting the transactions that they are aware the proceeds are illegal and tend to
 24 demonstrate a consciousness of guilt. If VINNIK believed he were conducting a legitimate money
 25 transmitting business, or digital currency exchange, he would have no reason to take elaborate steps to
 26 try to hide the true source of these funds through shell companies and in overseas bank accounts.

27
 28 ⁷ A proxy is one that masks a user’s true IP address with another in order to conceal their
 whereabouts or internet usage, which I know to be very popular with cybercriminals.

Witness G

42. Witness G is

REDACTED

REDACTED

43. According to Witness G, Mt. Gox was an original digital currency exchange, founded in San Francisco, California, and then relocated to Tokyo, Japan. Based on review of records, between 2011 and 2014, Mt. Gox suffered a series of computer intrusions, or “hacks,” that contributed to Mt. Gox failing and declaring bankruptcy in 2014.

Witness H

44. Witness H is an expert in the area of tracing digital currency by analyzing the blockchain and by using software designed to trace digital currency. Witness H analyzed the proceeds of the computer intrusion, or “hack,” of Mt. Gox that occurred between 2011 and 2014.

45. Witness H analyzed the various hacks of Mt. Gox and the movement of bitcoin out of Mt. Gox over a period of years. Witness H observed from records and analysis that the bitcoin that was stolen from Mt. Gox was eventually consolidated into several different accounts. Most of the funds stolen from Mt. Gox was eventually moved into accounts at BTC-e, at Tradehill, and back into Mt. Gox.

46. Witness H observed that the accounts receiving the stolen bitcoin were associated with accounts controlled by the “wme” address, the “prepaid” address, and the “sidorov” address. In other words, VJNNIK was a controller of a majority of the stolen bitcoin from Mt. Gox.

Witness I

47 Witness I

REFACTED

REFACTED

23 48. Witness I reviewed records that reflect transactions of bitcoin through Tradehill that
24 have been linked to the thefts of bitcoin from Mt. Gox. Tradehill was based in San Francisco,
25 California, within the Northern District of California.

1

1 / 1

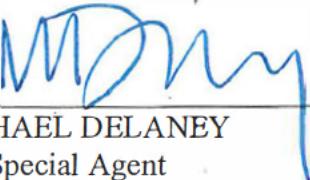
1

1 **Identification**

2 49. Alexander Vladimirovich VINNIK (also known as "WME") is a Russian citizen born on
3 REDACTED, in Kurgan, Russia. He is a white male with a medium build, brown eyes, and brown
4 hair. VINNIK maintains Russian Passport number REDACTED.

5 50. Attached to this affidavit as Exhibit 1 are photographs of VINNIK's current and
6 previous passport photographs, both of which were obtained from VINNIK's personal email account,
7 wmewme@gmail.com, and Hyatt Hotels Corporations. Based upon my investigation as described in
8 summary detail hereinabove, I have confirmed that the attached photographs are of Alexander
9 Vladimirovich VINNIK, who is charged in this case.

10 Executed this 9th day of August, 2017, at San Francisco, California, United States of America.

11 
12 MICHAEL DELANEY
13 HSI Special Agent

14 Signed and sworn to before me this 9th day of August, 2017, at San Francisco, California.

15 
16 HONORABLE RICHARD SEEBORG
17 UNITED STATES DISTRICT JUDGE

1
2
3
4
5
6
7
8
9
EXHIBIT 1
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28



P<RUSVINNIK<<ALEXANDER<<<<<<<<<<<<<<<<<

REDACTED

<<<<<<<<<<<<00



REDACTED

